CITED REF. 4

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平9－307544

(43)公開日　平成９年(1997)11月28日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ　9/10			Ｈ０４Ｌ　9/00	６２１Ａ	
Ｇ０６Ｋ　19/10		7259－5Ｊ	Ｇ０９Ｃ　1/00	６４０Ｄ	
Ｇ０９Ｃ　1/00	６４０	7259－5Ｊ		６４０Ｂ	
			Ｇ０６Ｋ　19/00	Ｒ	
Ｈ０４Ｌ　9/32			Ｈ０４Ｌ　9/00	６７５Ｂ	

審査請求　未請求　請求項の数４　ＯＬ　（全７頁）

(21)出願番号　特願平8－122071

(22)出願日　平成８年(1996)５月16日

(71)出願人　000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番２号

(72)発明者　村田　祐一
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(72)発明者　林　誠一郎
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

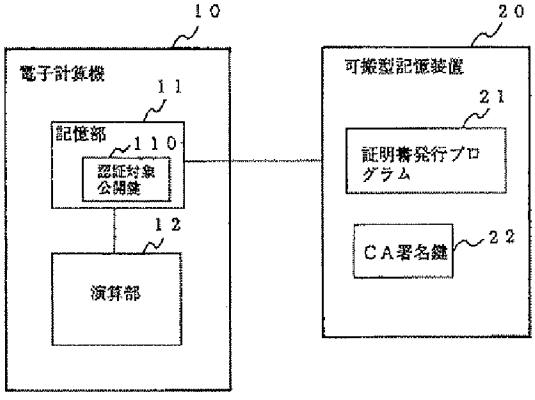
(74)代理人　弁理士　鈴木　誠

(54)【発明の名称】　可搬型暗号鍵認証システム

(57)【要約】

【課題】　証明書発行機能か不正使用されない高セキュリティを実現しつつ、認証対象者の電子計算機での証明書発行を可能にする。

【解決手段】　証明書発行プログラム２１と証明書発行権者（ＣＡ）の署名鍵２２を可搬型記憶装置２０に格納し、該記憶装置２０を電子計算機１０と切り離してＣＡに保持せしめる。証明書発行時、ＣＡは記憶装置２０を電子計算機１０に接続し、証明書発行プログラム２１とＣＡ署名鍵２２を電子計算機１０に転送する。電子計算機１０は、該証明書発行プログラムにより、ＣＡ署名鍵を用いて、認証対象公開鍵１１０に対するＣＡの証明書を生成する。なお、電子計算機１０と可搬型記憶装置２０の構成の一部又は全部を可搬型電子計算機としてもよい。



1

【特許請求の範囲】

【請求項１】　可搬型の記憶装置と該可搬型記憶装置を接続可能な電子計算機とで構成される可搬型暗号鍵認証システムにおいて、

前記可搬型記憶装置は証明書発行プログラムと証明書発行権者（ＣＡ）が証明書を発行する際に用いるＣＡ署名鍵を保持し、前記電子計算機の記憶部は認証対象者の公開鍵を保持し、

証明書発行時に、前記可搬型記憶装置を前記電子計算機に接続して、前記証明書発行プログラムとＣＡ署名鍵を前記電子計算機の記憶部に転送し、前記電子計算機の記憶部で保有する認証対象者の公開鍵に対して、電子計算機の演算部により証明書発行処理を行うことを特徴とする可搬型暗号鍵認証システム。

【請求項２】　前記可搬型記憶装置は、証明書発行プログラムとＣＡ署名鍵に加えて、暗号鍵生成プログラムを保持し、

証明書発行時に、前記電子計算機の演算部では、認証対象者の公開鍵を生成し、該生成した公開鍵に対して証明書発行処理を行うことを特徴とする請求項１記載の可搬型暗号鍵認証システム。

【請求項３】　記憶部と演算部を持つ可搬型の第１の電子計算機と、該第１の電子計算機に接続可能な第２の電子計算機とで構成される可搬型暗号鍵認証システムにおいて、

前記第１の電子計算機の記憶部は、証明書発行プログラムとＣＡ署名鍵を保持し、前記第２の電子計算機の記憶部は、認証者の公開鍵を保持し、

証明書発行時に、前記第１の電子計算機を前記第２の電子計算機に接続して、前記第２の電子計算機の記憶部から認証対象者の公開鍵を前記第１の電子計算機の記憶部に転送し、前記第１の電子計算機の記憶部で保有する証明書発行プログラムとＣＡ署名鍵を用いて、該第１の電子計算機の演算部で認証対象者の公開鍵に対する証明書発行処理を行い、該発行した証明書を第２の電子計算機の記憶部へ転送することを特徴とする可搬型暗号鍵認証システム。

【請求項４】　前記第１の電子計算機の記憶部は、証明書発行プログラムとＣＡ署名鍵に加えて、暗号鍵生成プログラムを保有し、

証明書発行時に、前記第１の電子計算機の演算部が暗号鍵生成処理を行い、生成した公開鍵に対して、証明書発行処理を行うことを特徴とする請求項３記載の可搬型暗号鍵認証システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、情報セキュリティ技術の暗号認証機能を公開鍵暗号方式を利用して実現する場合に、可搬型の記憶装置や電子計算機を使用して公開鍵を認証するシステムに関するものである。

2

【０００２】

【従来の技術】従来、公開鍵暗号方式を用いて暗号認証機能を実現する際には、認証センタ（＝証明書発行権者、Certification Authority：ＣＡ）を設置し、認証対象者の公開鍵に対してＣＡから発行される認証書によって公開鍵の正当性を保証するという方式がとられていた。証明書とは具体的には、公開鍵の署名対象情報としてＣＡの署名鍵を用いて生成されるディジタル署名である。

【０００３】また、ＣＡが、鍵を生成する機能を持ち、鍵生成と証明書発行の両方を行う場合もある。

【０００４】

【発明が解決しようとする課題】従来技術においては、ＣＡが保持する証明書発行プログラムが第三者に不正使用されないように厳密にセキュリティ対策をこうじる必要があった。また、ＣＡの証明書を発行してもらうために、各認証対象者は自分の公開鍵をオンラインもしくはオフラインでＣＡに提出しなければならなかった。

【０００５】本発明の目的は、ＣＡ機能が不正使用されないように高いセキュリティを実現しながら、認証対象者の電子計算機において証明書発行を可能にするような可搬型暗号鍵認証システムを提供することにある。

【０００６】

【課題を解決するための手段】請求項１の発明では、証明書発行プログラムとＣＡ署名鍵を可搬型記憶装置に格納し、該可搬型記憶装置は、認証対象者の公開鍵を保持する電子計算機と切り離してＣＡが保持する。これにより、証明書発行プログラムとＣＡ署名鍵の不正使用を防ぐと同時に、認証対象者の電子計算機に該可搬型記憶装置を接続することにより、認証対象者の電子計算機上で証明書発行処理が行えるようになる。したがって、認証対象者が自分の公開鍵をＣＡに提供する必要がなくなる。

【０００７】また、請求項２の発明では、暗号鍵生成プログラムも可搬型記憶装置上に保有し、認証対象者の暗号鍵生成もＣＡが行うことを要旨とする。

【０００８】請求項３の発明では、証明書発行プログラムとＣＡ署名鍵を可搬型の第１の電子計算機の記憶部に格納する。この可搬型の第１の電子計算機を、認証対象者公開鍵を保持する第２の電子計算機と切り離してＣＡが保持することにより、証明書発行プログラムとＣＡ署名鍵の不正使用を防ぐと同時に、第２の電子計算機に第１の電子計算機を接続のうえ、該第１の電子計算機の演算部で証明書発行処理が行えるようになるため、認証対象者が自分の公開鍵をＣＡに提供する必要がないのに加え、証明書発行プログラムとＣＡ署名鍵が第１の電子計算機の外部に出ることがないため、さらに安全に証明書発行処理が行える。

【０００９】また、請求項４の発明では、暗号鍵生成プログラムも可搬型の第１の電子計算機の記憶部に保有

し、認証対象者の暗号鍵生成も該第１の電子計算機の演算部で行うことを要旨とする。

【００１０】

【発明の実施の形態】以下、本発明の各実施例について図面により説明する。

【００１１】〈実施例１〉図１は本発明の第１の実施例の一構成図で、１０は電子計算機、２０は可搬型記憶装置である。なお、可搬型記憶装置２０の例としては、ＰＣＭＣＩＡインタフェースを有するＰＣカード、ＩＣメモリカード、フロッピディスク等が考えられる。可搬型記憶装置２１は、その内部に証明書発行プログラム２１とＣＡが証明書を発行するために用いるＣＡ署名鍵２２を保有し、電子計算機１０とは独立してＣＡが保持しておく。電子計算機１０は記憶部１１と演算部１２からなり、認証対象者は、証明書を発行してもらいたい認証対象公開鍵１１０を記憶部１１で保持する。

【００１２】証明書発行時、ＣＡは可搬型記憶装置２０を電子計算機１０に接続し、証明書発行プログラム２１とＣＡ署名鍵２２を電子計算機１０の記憶部１１に転送する。電子計算機１０の演算部１２は、この証明書発行プログラム２１を用いて証明書発行処理を行う。

【００１３】図２は、電子計算機１０の演算部１２における証明書発行処理の概要を示したものである。すなわち、記憶部１１に格納された認証対象公開鍵１１０を証明書発行情報として証明書発行プログラムに与え、ＣＡ署名鍵を用いて、認証対象公開鍵１１０に対するＣＡの証明書を生成する。該生成した証明書は記憶部１１へ格納する。

【００１４】〈実施例２〉図３は本発明の第２の実施例の構成図である。これは、図１の第１の実施例の可搬型記憶装置２０の内部に保有しておくものとして、暗号鍵生成プログラム２３を追加したものである。可搬型記憶装置２０は電子計算機１０とは独立してＣＡが保持しておく。

【００１５】証明書発行時、ＣＡは可搬型記憶装置２０を電子計算機１０に接続し、証明書発行プログラム２１、ＣＡ署名鍵２２、および暗号鍵生成プログラム２３を電子計算機１０の記憶部１１に転送する。

【００１６】電子計算機１０の演算部１２においては、まず、暗号鍵生成プログラムを動作させ、認証対象者の暗号鍵を生成する。生成した暗号鍵は記憶部１１に保持する。続いて演算部１２において、図２で示す証明書発行処理を行う。すなわち、記憶部１１で保持された暗号鍵のうち、認証対象公開鍵を証明書発行情報として証明書発行プログラムへ入力として与え、ＣＡ署名鍵を用いて、認証対象公開鍵に対するＣＡの証明書を生成する。生成した証明書は記憶部１１へ格納する。

【００１７】〈実施例３〉図４は、本発明の第３の実施例の構成図で、１０は第２の電子計算機Ｂ、３０は第１の可搬型電子計算機Ａを示すものである。なお、可搬型電子計算機Ａ３０の例としては、ＣＰＵを持つＩＣカードが考えられる。該可搬型電子計算機Ａ３０の記憶部３１に、証明書発行プログラム３１１とＣＡ署名鍵３１２を保持する。該可搬型電子計算機Ａ３０は電子計算機Ｂ１０とは独立してＣＡが保持しておく。電子計算機Ｂ１０の構成は図１の実施例と同様である。

【００１８】証明書発行時、ＣＡは可搬型電子計算機Ａ３０を電子計算機Ｂ１０に接続する。認証対象者は、電子計算機Ｂ１０の記憶部１１内の証明書を発行してもらいたい認証対象公開鍵１１０を可搬型電子計算機Ａ２３０記憶部３１へ転送する。そして、該可搬型電子計算機Ａ３０の演算部３２において、図２で示す証明書発行処理を行う。すなわち、記憶部３１に転送された認証対象公開鍵を証明書発行情報として証明書発行プログラム３１１に入力として与え、ＣＡ署名鍵３１２を用いて、認証対象公開鍵に対するＣＡの証明書を生成する。該生成した証明書は電子計算機Ｂ１０の記憶部１１へ転送する。

【００１９】〈実施例４〉図５は、第４の実施例の構成図である。これは、図４の第３の実施例における第１の可搬型電子計算機Ａ３０の記憶部３１に保有しておくものとして、暗号鍵生成プログラム３１３を追加したものである。該可搬型電子計算機Ａ３０は第２の電子計算機Ｂ１０とは独立してＣＡが保持しておく。

【００２０】証明書発行時、ＣＡは可搬型電子計算機Ａ３０を電子計算機Ｂ１０に接続する。そして、まず、該可搬型電子計算機Ａ３０の演算部３２において、暗号鍵生成プログラム３１３を動作させ、認証対象者の暗号鍵を生成する。該生成した暗号鍵は記憶部３１に保持する。続いて、該可搬型電子計算機Ａ３０の演算部３２において、図２で示す証明書発行処理を行う。すなわち、記憶部３１で保持された暗号鍵のうち、認証対象公開鍵を証明書発行情報として証明書発行プログラム３１１へ入力として与え、ＣＡ署名鍵３１２を用いて、認証対象公開鍵に対するＣＡの証明書を生成する。最後に、生成した証明書を電子計算機Ｂ１０の記憶部１１へ転送する。

【００２１】

【発明の効果】以上説明したように、本発明によれば、認証対象者の公開鍵に対する証明書発行機能を可搬型記憶装置もしくは可搬型電子計算機に格納し、それらをＣＡが管理することで不途使用を防ぐことが可能になり、さらにそれらの可搬型記憶装置、もしくは可搬型電子計算機を認証対象者の電子計算機に接続して証明書発行処理が可能になるため、認証対象者が自分の公開鍵をＣＡに提出しなくても証明書を発行してもらうことが可能になる。

【図面の簡単な説明】

【図１】本発明の第１の実施例の構成図である。

【図２】証明書発行プログラムの動作概要を示す図であ

5

る。

【図３】本発明の第２の実施例の構成図である。

【図４】本発明の第３の実施例の構成図である。

【図５】本発明の第４の実施例の構成図である。

【符号の説明】

１０　電子計算機

１１　記憶部

１１０　認証対象公開鍵

１２　演算部

２０　可搬型記憶装置

6

＊２１　証明書発行プログラム

２２　ＣＡ署名鍵

２３　暗号鍵生成プログラム

３０　可搬型電子計算機

３１　記憶部

３１１　証明書発行プログラム

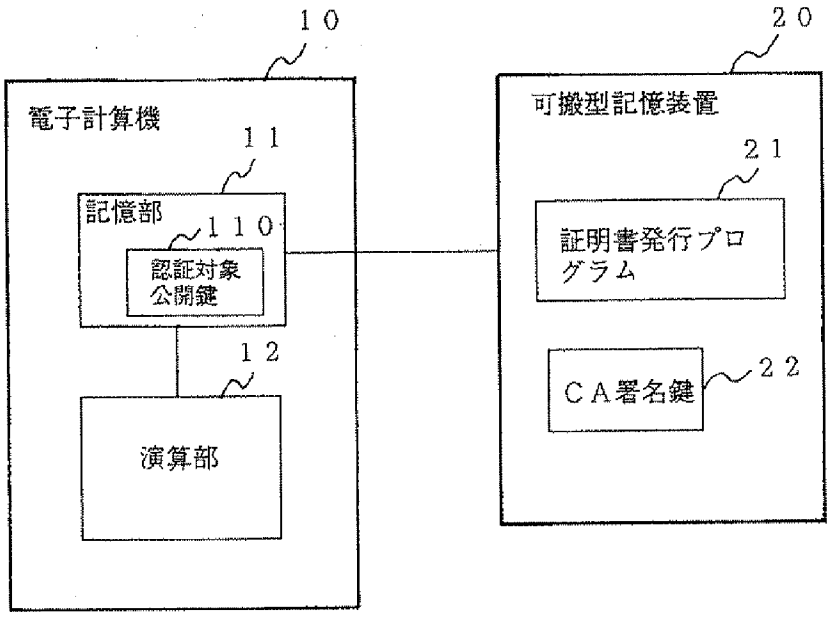
３１２　ＣＡ署名鍵

３１３　暗号鍵生成プログラム

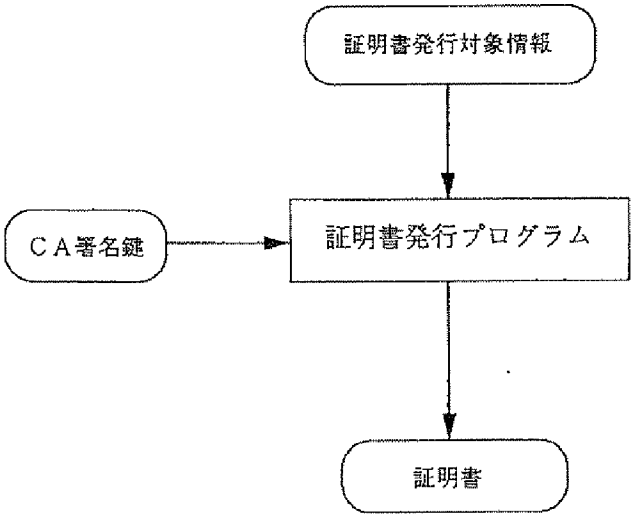
３２　演算部

＊10

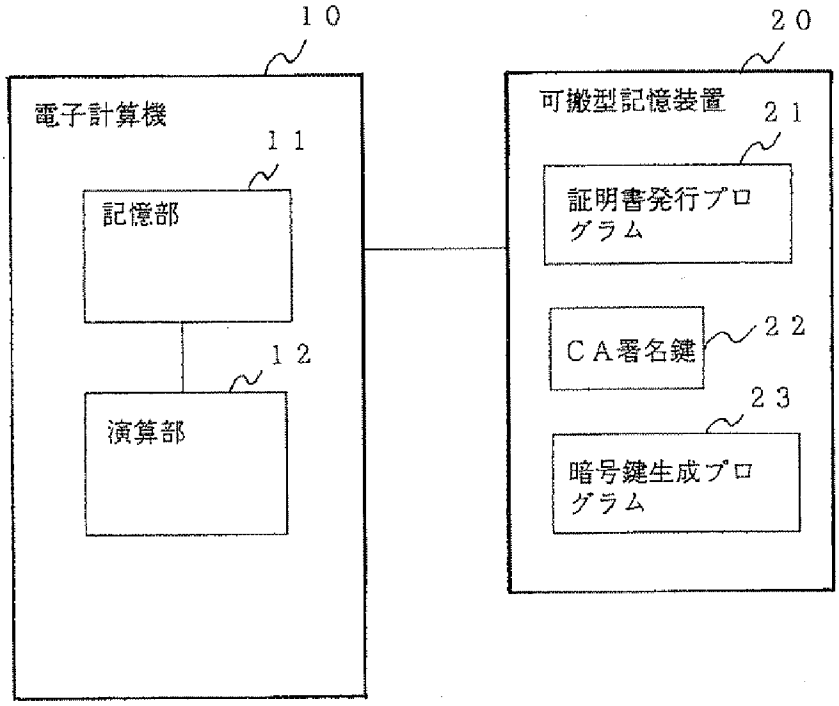
【図１】



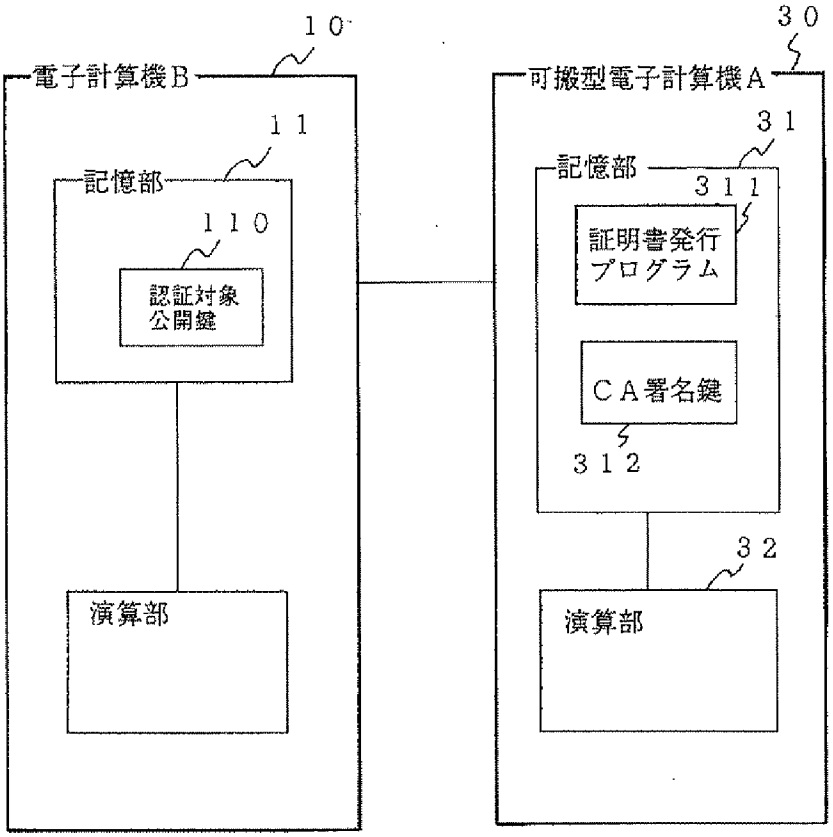
【図２】



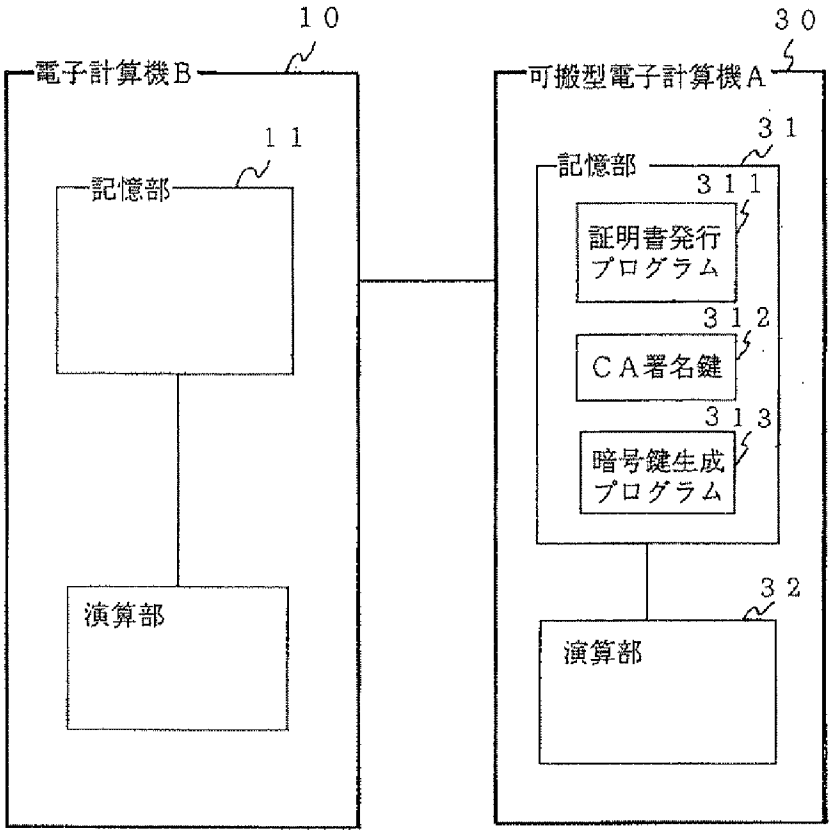
【図3】


10
電子計算機
11
記憶部
12
演算部
20
可搬型記憶装置
21
証明書発行プログラム
22
CA署名鍵
23
暗号鍵生成プログラム

【図4】


10
電子計算機B
11
記憶部
110
認証対象
公開鍵
演算部
30
可搬型電子計算機A
31
記憶部
311
証明書発行
プログラム
CA署名鍵
312
32
演算部

【図5】


10
電子計算機B
11
記憶部
演算部
30
可搬型電子計算機A
31
記憶部
311
証明書発行
プログラム
312
CA署名鍵
313
暗号鍵生成
プログラム
32
演算部